Author(s): Azenabor, Cyril E.; Shoniregun, Charles A.; Imafidon, Chris
Title: e-Government security implications
Year of publication: 2009
Citation: Azenabor, C.E., Shoniregun, C.A., Imafidon, C. (2009) 'e-Government security implications' Proceedings of Advances in Computing and Technology, (AC&T) The School of Computing and Technology 4th Annual Conference, University of East London, pp.167-176
Link to published version:
http://www.uel.ac.uk/act/proceedings/documents/FinalProceedings.pdf

E-GOVERNMENT SECURITY IMPLICATIONS

Cyril E. Azenabor, Charles A. Shoniregun and Chris Imafidon
University of East London, United Kingdom
cyrillicehi@yahoo.com, c.shoniregun@uel.ac.uk, c.o.imafidon@uel.ac.uk

Abstract: The electronic government (e-Government) is mainly concerned with providing quality services and value added information to citizens, and it has potentials to build better relationships between government and the public by making interactions between citizens and government agencies smoother, easier, and more efficient. The use of Internet medium has helped government organisations and non-government organisations to increase their productivity, reduce costs and also improve services. The most security implications in e-government is the protection of the data security, whereby the privacy of the citizens are not guaranteed, because the access to the data are not controlled by authorised agents, and due to human interaction it is vulnerable to so many attacks. Hackers developed sneaky ways attacking the digital communicating system by phishing into the information systems. There are problems about security vulnerability in government websites, which has made the public to be extremely concerned, and third party routinely invade government websites for fraudulent purposes. Attitudes of people interrogating this system will go a long way by having a strong principle of sincerity and honesty so as to help rectifying the security issues and strict legislative rule cannot be undermined in dealing with offenders. This paper proposed a model of five blocks of steps to bring security in e-Government systems.

1. Introduction:

Information technology has become a fundamental part of government activities, and will continue to be essentially important to administration, decision-making and direct services delivery. It will also be decisive in the gradual relationships between government and other kinds of organisations, and between government and citizens. Government has been in the forefront of information technology research for quite sometime, it has been known that social security and national defence operates by depending solely on information technology. The digital communications and advance networking offer some great value to government functions in Internal Revenue service e-file and telefile programmes by allowing taxpayers to file their returns electronically making use of modern day electronic technology. Digital technologies have been used to transform government operations so as to improve its effectiveness, efficiency, as well as service delivery. The e-Government is mainly concerned with providing quality services and value-added information to citizens, it has the potentials to build better relationships between government and the public by making interactions between citizens and government agencies smoother, easier, and more efficient and in this respect, e-Government serves a similar purpose to customer relationship management in business world, therefore government still lack the fundamental infrastructure, organisational culture, and resources required for the transformation of e-Government.

2. Effective e-Government programme:

An effective e-Government programme requires successful seamless interaction of appropriate Information and Communication Technology (ICT), quality information, engaged public employees, good administrative process, and government leadership (Lee et. al, 2005). Government units at national, regional and local levels around the world are applying information technologies vigorously. The application of Information Technology (IT) to government service is often termed "e-Government" and the larger concept of government that depends upon IT to achieve basic missions is termed "digital government", this distinction is of course, lexically arbitrary, but serves to distinguish Relational Database (R&D) specifically aimed at creating techniques for applying IT to government operations. Such R&D efforts also consider the long-term impact of these applications on citizens and government itself (Marchionin et al, 2003). The e- government refers to the use of ICTs to promote more efficient and effective government services, allow greater public access to information and make government more accountable to citizens and e-Government initiatives are common in most developed countries including industrialised economics, emerging economics as well as developing economics (Punia and Saxena, 2004). Information technology is already an essential part of government operations and will continue to be vitally important to administration, decision making, and direct service delivery. It will also be critical in the evolving relationships between government and other kinds of organisations, and between government and citizens (Dawes et al., 1999). Government organisations from national legislatures to local social services agencies operate in a complex and increasingly globalise economic and political system and are not immune from these shifts, especially as they relate to the use of information technologies in their work (Clift, 2002). Governments are not using information technology to run its activities only, but also to get itself involve in electronic commerce (e-Commerce). 'There is no doubt that electronic commerce is going to have a profound effect on business, government and consumers and on the way people live and work. The e-Commerce presents enormous challenges' (Shoniregun, 2005). Despite all these activities by the governments in running electronic information to partake in e-Commerce and to better the society, the greatest challenges to the governments is the short fall in online information security.

3. E-Government management:

The security issues in information systems are very problematic and difficult to solve. The use of the Internet medium has helped government and non-government organisations to increase their productivity, reduce costs and also improve services. Information systems are attacked on a daily basis as a result of such attacks billions of dollars has been loss. Furthermore, based on recent computer crime and security survey, the theft of proprietary remains the highest losses that have ever been recorded in history, other forms include unauthorised access, telecom fraud, financial fraud, viruses, laptop theft, insider Internet abuse, denial of service (DOS) attacks, sabotage, system penetration, telecom eavesdropping and active wiretapping (West, 2002). The security lapse in e-service requires the verification of the computer server, which authenticates the integrity of the message, confidentiality and privacy associated with

the transmission of the information. Although the authentication of the user is also desirable, simple user authentication mechanisms such as passwords are cost-effective for most of these applications (Luna-Reyes and Gil-Garcia, 2003). Servers transacting information and communications are at security risk and more attractive targets to attackers. The most security issues in e-Government management are the protection of the data integrity, whereby the privacy of the citizens is not guaranteed, because authorised agents do not control the access to the data. Human interaction cannot be undermined in this case, hence its vulnerabilities such as imperfect designs, bad programming practices and user decisions. One of the greatest problems in (e-Government) is the nature and manner in which the information technology facilities are being run. It has been observed in some countries that the networks transmitting confidential information is no longer in use hence there is lack of innovation, therefore they are too old to carry out some basic security protection of its data, and many employees do not have access to the web.

4. Government Information and Services:

The e-Government information security is not controlled because of some lapses which made unauthorised people to have access into its data and data integrity is not maintained. There is danger to individual rights and privacy because everyone seems to have access into the electronic world, while exposing personal information of its citizens. The involvement of government in electronic information to improve the life of its citizens is a welcome development, but allowing public access to government information and services at anytime and from anywhere around the world has undermined the security of individual which is against the data act protection. The fraudulent transactions in the electronic system will hardly made the public to have any trust in dealing with the government in the area of electronic business whereby they refuse to disclose their details to the social security systems or using credit or debit card when paying their bills online to the government and its agencies. There is no privacy in the e-Government and neither do we have security in the data, most of the government agencies publicly provide all available data about its citizens, so as to develop, study, analyse policy and legislation of benefit to its citizenry. The use of the Internet to acquire data from the citizenry more efficiently and at lower cost is a natural approach being considered by many countries. However, such an approach creates deep concerns about authenticity of the respondents who may answer online, and the opportunity this may create for fraud and for the invasion of privacy by the inadvertent leakage of Personal Identifiable Information (PII) may be revealed to unauthorised third pasties (Stolfo et al. 2003).

Accessing government websites is tantamount to privacy risks, and if government do not find solution to these inherent problems, it will always attract third parties to this website to carry out their fraudulent activities by making use of private data and queries. The Internet stands as a channel or medium between government and its citizens and fraudsters capitalise on it to sniff into people's data to carry out their nefarious act. This act has created a great concern in the minds of the public and has prompted government to be security conscious, and as far as there are human interactions, there will be no absolute security. There have been a lot of invaders who hacks into government computer

systems by penetrating through government and its agencies network systems for their selfish reasons. Despite the sophisticated security technology network to protect some government networks infrastructure, hackers developed a sneaky way attacking the digital communicating system by phishing into their information systems. The fact is that government has not folded its hands in dealing with the situation, a huge amount of money has been spent to arrest the situation by setting up some security software systems which was installed to continuously observed traffic in order to detect attempts to penetrates computer servers by hackers with malicious act and the computer fraudsters always have their way breaking into the security systems. Studies shows that there is a great security problem about communication in government websites which has made the public to be extremely concerned, and the issue is mainly on the third party who routinely invade government websites day in and day out for fraudulent purposes. For this reason, citizens are always conscious and concerned about the security and privacy of their personal data both in commercial communication and government websites because of uncertainty. Not withstanding, government websites have secured portals as a means of safety to prevent them from invaders, still hackers will always break into the system.

The phishers also build camouflage websites in disguise in order to look like that of governments and its agencies' sites, when the public log into these sites, they use the information and data of the citizens in committing fraud. Phishing involve a trap laid for unwary computer users who received spoofed (fake) e-mails or visit fraudulent websites and are fooled into divulging financial data such as credit card numbers, account user names and passwords, social security numbers, etc., according to Anti-phishing Working Group, (Trembly, 2005). Governments itself could also give its security agents unlimited access to organisations' computer system which is in violation of privacy law. A case in point was the 9/11 attacks and the US President authorised the domestic surveillance of individuals suspected of contacting terrorists without court approval. The government intends to assert military and state secrete privilege that permits the government to protect against unauthorised disclosure in litigation of information that may harm national security interests (Hills, 2006).

5. Security threats:

Information security at major government agencies have shown that government systems were not being adequately protected from computer-based threats, as these systems process, store, and transmit enormous amount of sensitive data and are indispensable to many government agency operations (Dacey, 2002). With this, it is shown that poor information security is a wide spread problem encounter by the government which has a potential wasteful effects. The level of risk as a result of security weaknesses is quite alarming because most of the government activities are supported by automated systems and electronic data, and its agencies would find it difficult and impossible to carry out their daily routine without these information assets. Dacey (2002), outlined the weaknesses identified by government operations and the assets at risks as follows:

- Resources, such as federal and collections, could be lost or stolen.
- Computer resources could be used for unauthorised purposed or to launch attacks on others.
- Sensitive information, such as taxpayer data, social security

records, medical records, and proprietary business information, could be inappropriately disclosed or browsed or copied for purposes of espionage or other types of crime.

- Critical operations, such as those supporting national defence and emergences, could be disrupted.
- Data could be modified or destroyed for purposes of fraud or disruption.
- Agency mission could be undermined by embarrassing incidents that result in diminishing confidence in their ability to conduct operations and fulfil their fiduciary responsibilities.
- A lack of senior management attention to information security.
- Inadequate accountability for job and programme performed related to information technology security.
- Limited security training for general users, information technology professionals and security professionals.
- Inadequate integration of security into the capital planning and investment control process.
- Poor security for contractor, provided services.
- Limited capability to detect, report, and share information on vulnerabilities or to detect intrusions, suspected intrusions, or virus infections.

Yang et al. (2005) further suggested that security problem of e-Government are:

- The security question caused by attacking maliciously or the virus propagating, the security question caused by data let out or users verified.
- The security leak that one's own human factor causes is the greatest potential safety hazard of the whole network, for instance the network is let out.
- Illegal personnel operate network equipment or resources illegally, or legal users go beyond one's commission to use the resources of the network.
- Sensitive information is eavesdropped, or let out in the course of transmitting; information is lost or stolen in storing the medium.
- The integrity of the data is destroyed, delete, add, revise and operate to data maliciously for the data using right that is obtained illegally, interfere the normal use of legal users.
- Attack of the denial of service, interfere network service system, change its working procedure, execute irrespective procedure to slow down system response and cause system paralysis even.
- Utilise network promulgate virus, the kind of computer virus increasing with the geometric progression, the overflowing of virus brings the calamitous consequence to computer system. The polarisation of the network became the most important carrier that virus spread extensively, increases very great degree of difficult for the measuring and elimination of the virus at same time.
- Fragile with inherent network system, security of adopted Internet protocol (IP) network extensively of development at full speed is not obviously strengthened at present,

such as (IP) address relying on the software to dispose is very easy to imitated or cheated.

- Security question of equipment or the circuit, the cutting off of communication line, the trouble of the interconnected equipment itself of network may endanger the integrality of data transmission seriously too.

According to Li (2005) study based on China, the problems in the development of e-Government, has to do with security that has become the key problem in government information, which influences greatly on the development of e-Government. Compared with e-Commerce the government has higher demands for the security information. The capability in research and development of information technology in China is relatively weak, which challenges to some extent the development of e-Government. Therefore security has become the top issue in developing e-Government. Only safe products and technology enable to provide security guarantee for government information and also legislation in Chinese e-Government lags relatively behind the developing countries, which to a great extent affects the development of e-Government. Many developed countries have already established a series of regulations, laws to improve their e-Government. Electronic signature is allowed to be use, e-payment is acceptable legally, and some network security policies are published. Though the "Electronic Signature Law of People's Republic of China" has been accepted legally since 2004, more laws and regulations related with e-Government to guide the electronic transactions and e-payment, and to protect the safety of databases. But some of the information technology infrastructures used by some government are obsolete, cumbersome and dilapidated. E-voting is another aspect of security decadence in e-Government and a lot of attention should be paid to this.

6. E-voting:

The human interaction in electronic system makes it vulnerable to so many attacks. Of all the services rendered by e-Government through the electronic information system, e-voting has a delicate set of security requirements. Record shows that e-Democracy applications which has to do with e-Government are highly at security risks and most vulnerable. The cost of protection is very high in estimation. Though, the current development of software and hardware cannot fully provide adequate and acceptable level of security for this kind of application. Despite all the technological advances everywhere it is being used, there has not been a complete secure e-voting solution. In the past there has been multiple-channel voting and there are still occurrences of these across the globe where Internet or electronic voting systems is being practised, and technological advancement have not been able to provide a completely secure e-voting solution.

Xenakis and Macintosh (2004) outlined some cases of procedural security lapses in e-voting which have been documented and grouped into the following generic areas:

- The lack of procedures to control the activities of commercial vendors and government officials before and during the election, providing an audit trial of their actions.
- Existing measures of procedural security, which are inadequate to cover all aspects of the electoral process such as the verification of voter providing data, the secure dissemination of voter credentials

and the prevention of double voting through multiple voting channels.

- The lack of agent compliance to existing measures of procedural security.

Mote (2001) report of the National Workshop on Internet Voting discussed some security issues in adopting e-voting which says that remote Internet voting systems pose significant risk to the integrity of the process, and should not be fielded for use in public elections until substantial technical and social security issues are address. The security risks associated with these systems are both numerous and pervasive, and in many cases, cannot be resolved using even today's most sophisticated technology. Internet-based voter registration poses significant risk to the integrity of the voting process, and should not be implemented until adequate authentication infrastructure is available and adopted. Online registration without the appropriate security infrastructure would be at high risk for automated fraud, that is, the potential undetected registration of large numbers of fraudulent voters. This is because computer-based voting systems as well as other distributed computing systems are vulnerable to attack at three main points, the server, the client and the communication path. The current hardware and software architectures, a malicious payload on a voting host can actually change a voter's vote without the voter or anyone else noticing, regardless of the encryption or voter authentication in place, because the malicious code can do its damage before the encryption and authentication is applied to the data, and the malicious module can then erase itself, so no evidence of fraud is left behind to correct or even detect (Rubin, 2002).

7. Discussion:

The e-Government systems are highly expensive to run with many associated risks, but the most difficult to handle among these risks are the technological risk and this is mainly concerned with security. Carbo and Williams (2004) proposed a model on security by using Pennsylvania as a case study and they developed survey instrument by collecting data from appropriate constituent's populations. For government entities the survey will include what functions and services they have currently implemented for e-Government services, what they are planning for new services, the process used to make their system reality, how security and privacy issues have affected their systems, how citizens have been involved, and what metrics they have gathered about current e-Government.

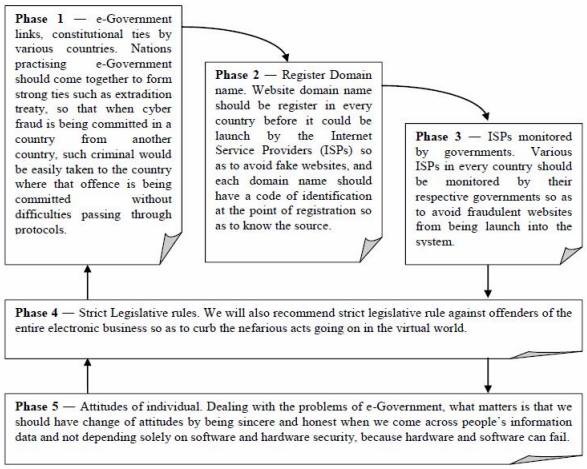

Figure1: Five phases of securing e-Government systems model

Providing a survey cannot solve the problem of security system, what matters is to provide a solution. A survey can only highlight the course of a problem and the source, it cannot bring solution and what we need is solution. On the other hand, previous study by Elkins and Wilson (2001)

discussed about IPSec (Internet Protocol Security) when used, third party hosts cannot intercept and decode data protected by IPSec. That cryptographic device can be replaced by a proper IPSec implementation. This is purely not true and cannot work because some penetration attack, which involve malicious payload, mentioned above could target host of a Trojan horse and when executed can cause security damages without detection and IPSec cannot stop this and the likes of it. The developed nations who have promulgated all types of legislative laws, like e-payments and others to protect e-Government electronic transactions and biometric design to protect them against fraud are still having security problems. Due to interactions of the systems by human beings, we will always encounter security issues in e-Government. On the other hand, who is going to interrogate the system? They are humans coming from different background and with different belief and principles guiding them. Are the people 100 percent trusts worthy? No matter how secured the system could be in the electronic world, security problems will always raise its ugly head. We can only control it to a minimal even if we are very efficient in our security alertness. We presented our proposed five phases of securing e-Government systems model in figure1 above.

8. Conclusion:

There are urgent needs in changing of government policies where e-Government is to be adopted, so as to enhance more interaction among government agencies through database intercommunication or interaction. This is because the interaction of databases calls for a clear definition of information ownership and access. The involvement of government administrative in electronic business is a welcoming idea, but much has not been done to rectify the security problems and the electronic world has been treated with laxity. The security problem in the virtual world is a complex issue, even though there are many daily occurrences of information security breaches, therefore the government needs to continuously educating the public. The problems cannot be solved entirely by the government but collective effort of all stakeholders involved. We recommend that there should be incentive from the government so that workers such as the database administrators would not go out of their way to fraud the system.

9. References:

Carbo, T., and Williams, G. J. (2004), 'Models and Metrics for Evaluating Local Electronic Government Systems'. http://www.ejeg.com/volume-2/volume2-issue2/v2-i2-carbo-pp95-104.pdf (Accessed date: 23/06/06)

Clift, S. L. (2002), 'Transnational and Intergovernmental Electronic Communication: Policy Questions and Implications of the Emerging Global Information Network'. http://publicus.net/articles/transnational.html (Accessed date: 24/01/06)

Dacey, F. R. (2002), 'Information Security: Additional Actions Needed to Fully Reform Legislation' http://www.gao.gov/new.items/d02470t.pdf (Accessed date: 12/05/06)

Dawes, S. S., Bloniarz, A. P., and Kelly, L. K. (1999), 'Some Assembly Required: Building a Digital Government for the 21st Century'

http://www.ctg.albany.edu/publications/reports/some_assembly (Accessed date: 3/05/06)

Elkins, A., and Wilson, W. J. (2001), 'Security Issues in High Level Architecture Based Distributed Simulation' http://www.informs-cs.org/wsc01papers/107.PDF (Accessed date: 23/06/06)

Hills, F. (2006), 'U.S. Governments Sides With AT&T In Spying Lawsuit' http://proquest.umi.com/pqdweb?did=1029458251&sid=1&Fmt=3&clientId=13314&RQT=309&VName=PQD (Accessed date: 11/05/06)

Lee, M. S., Tan, X., and Trimi, S. (2005), 'Current Practices of Leading E-Government Countries' Communications of the ACM, Vol. 48, No. 10, Pgs. 99-104

Luna-Reyes, F. L., and Gil-Garcia, J. R. (2003), 'eGovernment & Internet Security: Some Technical and Policy Considerations' http://www.digitalgovernment.org/dgrc/dgo2003/cdrom/STUDENTS/lunareyes.pdf (Accessed date: 11/05/06)

Li, B. (2005), 'On the Barriers to the Development of e-Government in China' http://delivery.acm.org/10.1145/1090000/1089650/p549-li.pdf?key1=1089650&key2=8204801511&coll=GUIDE&dl=GUIDE&CFID=15151515&CFTOKEN=6184618 (Accessed date: 17/06/06)

Marchionini, G., Samet, H., and Brandt, L. (2003), 'Digital Government' Communications of the ACM, Vol. 46, No. 1

Mote, C.D. Jr. (2001), 'Report of the National Workshop on Internet Voting: Issues and Research Agenda'. http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/election2000/nsfe-voterprt.pdf

Punia, K. D., and Saxena, K. B. C. (2004), 'Managing Inter-organisational Workflows in e-Government Services' http://delivery.acm.org/10.1145/1060000/1052283/p500-punia.pdf?key1=1052283&key2=9855801511&coll=GUIDE&dl=GUIDE&CFID=15151515&CFTOKEN=6184618 (Accessed date: 24/05/06)

Rubin, D. A. (2002), 'Security Considerations for Remote Electronic Voting, Communications of the ACM, Vol. 45, No. 12

Shoniregun, C. A. (2005), ''Impacts and Risk Assessment of Technology for Internet Security: Enabled Information Small-Medium Enterprises. Publisher: Springer

Stolfo, J. S., Johnson, E., Pavlicic, T., and Jan, S. (2003), 'Citizen's Attitudes about Privacy While Accessing Government and Private Websites: Results of an Online Study' http://www.digitalgovernment.org/dgrc/dgo2003/cdrom/PAPERS/citsprivacy/stolfo.pdf (Accessed date: 14/05/06)

Trembly, C. A. (2005), 'Phishing Threatens Agents, Carriers, Insureds' National Underwriter. P&C. Erlanger: Vol. 109, No. 7, Pgs 2&11

West, C. B. (2002), 'Security Issues and Concerns in Electronic Government' Silver Spring: Vol. 16, No. 2, Pgs 1-15

Xenakis, A., and Macintosh, A. (2004), 'Procedural Security Analysis of Electronic Voting'

http://delivery.acm.org/10.1145/1060000/1052288/p541-xenakis.pdf?key1=1052288&key2=2148801511&coll=GUIDE&dl=GUIDE&CFID=70165127&CFTOKEN=30891626 (Accessed date: 14/05/06)

Yang, L., Lu, Y., and Fu, G. (2005), 'Study on e-Government Construction' http://delivery.acm.org/10.1145/1090000/1089649/p542-yang.pdf?key1=1089649&key2=6288801511&coll=GUIDE&dl=GUIDE&CFID=15151515&CFTOKEN=6184618 (Accessed date: 11/05/06)